Sub a1

WHAT IS CLAIMED IS:

1. A method of providing varying levels of security in a data processing system, the method comprising:

receiving information from an outside source;

retrieving an indicator from the received information that instructs the system to operate at a higher level of security;

preventing operation at a lower level of security until information is received by the system to authorize a decrease in security levels.

2. The method of claim 1 and further comprising:

receiving an encrypted message, said encrypted message comprising a Decreased-Security-Authorization-Code to authorize said decrease in security levels.

3. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in encryption/decryption levels.

4. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level.

5. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels.

6. The method of claim 2 wherein said encrypted message further comprises a key for use in a decryption algorithm.

7. The method of claim 6 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

8. The method of claim 1 and further comprising:

establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented by the system.

9. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of encryption/decryption that is being implemented by the system

10. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication that is being implemented by the system.

11. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication and a level of encryption/decryption that is being implemented by the system.

12. The method of claim 8 and further comprising:

configuring said Security Level Status Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels.

13. The method of claim 1 and further comprising:

utilizing a cable head-end as said outside source.

14. The method of claim 2 and further comprising using a Key Management Message to convey said Decreased Security Authorization Code.

15. The method of claim 14 wherein delivery of said Key Management Message is authenticated

16. The method of claim 14 wherein delivery of said Key Management Message is protected against a replay attack.

17. The method of claim 14 wherein delivery of said Key Management Message is authenticated and protected against a replay attack.

18. The method of claim 1 wherein a lower level of security is non-public Key mode, wherein a higher level of security is a public Key mode, the method further comprising:

continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source.

19. The method of claim 18 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

20. A method of providing a secure transition between security levels in a data processing system, the data processing system having at least a high level of security and a low level of security for operation, the method comprising:

using the system to receive information from an outside source;

operating the system at the high level of security;

continuing operation of the system at the high level of security until an encrypted authorization message is received by the system from the outside source authorizing a switch to a different level of security.

21. A cryptographic device comprising:

an input to receive a datastream;

a Security -Level-Status-Indicator; and

code means for executing a cryptographic algorithm wherein said cryptographic algorithm is indicated by said Security-Level-Status-Indicator.

22. The device as described in claim 21 wherein said code means for executing a cryptographic algorithm comprises code means for executing a high level cryptographic algorithm and code means for executing a low level cryptographic algorithm relative to said high level cryptographic algorithm.

23. The device of claim 22 wherein said high level cryptographic algorithm comprises a high level decryption algorithm and wherein said low level cryptographic algorithm comprises a low level decryption algorithm.

24. The device of claim 22 wherein said high level cryptographic algorithm comprises a high level authentication algorithm and wherein said low level cryptographic algorithm comprises a low level authentication algorithm.

25. The device of claim 22 wherein said high level cryptographic algorithm comprises a high level decryption algorithm and a high level authentication

algorithm and wherein said low level cryptographic algorithm comprises a low level decryption algorithm and a low level authentication algorithm.

26. The device as described in claim 22 wherein said high level cryptographic algorithm is a public Key encryption algorithm and wherein said low level cryptographic algorithm is a non-public Key encryption algorithm.

27. The device as described in claim 21 and further comprising code means for decrypting a Decreased Security Authorization Code.

28. The device as described in claim 27 and further comprising code means for preventing a replay attack in delivery of said Decreased-Security-Authorization-Code.

29. The device as described in claim 27 and further comprising a master key to use in decrypting said Decreased Security Authorization Code.

30. The device as described in claim 21 wherein said Security Level Status Indicator is encrypted.

31. A method of processing data comprising:

providing a receiver to receive a transmission;

establishing a Security-Level-Status-Indicator at said receiver;

establishing a first level of decryption at said receiver;

encrypting a first message at a first level of encryption;

transmitting said first message to said receiver at said first level of encryption;

receiving said first message at said receiver;

decrypting said first message encrypted at said first level of encryption;

transmitting a Decreased-Security-Authorization Code to change from said first level of decryption to a second level of decryption;

receiving said Decreased-Security-Authorization-Code;

determining a change in encryption level from said first level of encryption to said second level of encryption;

adjusting said Security-Level-Status-Indicator at said receiver;

encrypting a second message at said second level of encryption;

transmitting said second message at said second level of encryption;
receiving said second message at said receiver; and
decrypting said second message at said receiver.

32. An apparatus for processing data comprising:
a receiver to receive a transmission;
a Security-Level-Status-Indicator stored in said receiver;
first decryption code stored in said receiver for use in decrypting said transmission when encrypted at a first encryption level;
a transmitter to transmit said transmission;
first encryption code stored in said transmitter to encrypt a message at said first encryption level;
code means for transmitting a Decreased-Security-Authorization-Code from said transmitter to said receiver so as to change from said first level of encryption to a second level of encryption;
second decryption code stored in said receiver for use in decrypting said transmission when encrypted at said second level of encryption; and
second encryption code stored in said transmitter to encrypt at said second encryption level.